15-853: Algorithms in the real world — Assignment 2 (Cryptography and Optimization)

Due: Thursday Oct 28, 1999

Please feel free to send us email if there are any ambigouous questions.

Problem 1:

(a) Assuming p and q are primes, express $x^{-1} \bmod pq$ as a positive power of x.

(b) Given public key $e = 3$, $n = 391$ encode the value 45 using RSA.

(c) Assuming the same public key, decode the value 105 (you might want to write a short program to do it).

(d) In RSA for some n lets say $e = 3$ (a standard choice in some systems). If I accidentally give away d show how one can use this information to factor n.

Problem 2: Strang Chapter 8 problem 8.2.1.

Problem 3:
Consider the following problem

$$\begin{array}{ll} \text{maximize} & x_1 + x_2 \\ \text{subject to} & 2x_1 + x_2 \leq 4 \\ & x1, x2 \geq 0 \end{array}$$

(a) Starting with the initial solution $(x_1, x_2) = .1, .1$ solve this problem using the affine scaling interior-point method. You can assume that every step should take you 96% of the way to the boundary.

(b) Illustrate the progress of the algorithm on the the graph in $x_1 - x_2$ space.

Problem 4:
Let's say we augment linear programs to allow contraints to include absolute values (*e.g.* $|x_1| + 3|x_2| \leq b$). Can we solve all such problems in polynomial time? Show why or why not. (Assume $P \neq NP$.)

Problem 5:
Let $S = \{x \in R^n : Ax \leq b\}$ and $T = \{x \in R^n : Bx \leq d\}$. Assuming that S and T are nonempty, describe a polynomial time algorithm (in n) for checking whether $S \subset T$.

Problem 6:
Solve the following problem using the implicit enumeration branch-and-bound technique (the 0-1 programming technique) describe in class.

$$\begin{array}{ll} \text{minimize} & 3x_1 + 2x_2 + 5x_3 + x_4 \\ \text{subject to} & -2x_1 + x_2 - x_3 - 2x_4 \leq -2 \\ & -x_1 - 5x_2 - 2x_3 + 3x_4 \leq -3 \\ & x_1, x_2, x_3, x_4 \text{ binary} \end{array}$$